(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
8 February 2001 (08.02.2001)

PCT

(10) International Publication Number
WO 01/09701 A1

(51) International Patent Classification[7]: G06F 1/00

(21) International Application Number: PCT/US00/20267

(22) International Filing Date: 25 July 2000 (25.07.2000)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
09/366,654 3 August 1999 (03.08.1999) US

(71) Applicant and
(72) Inventor: MOHSEN, Amr [US/US]; 16348 Aztec Ridge Drive, Los Gatos, CA 95032 (US).

(74) Agents: GLENN, Michael, A. et al.; Glenn Patent Group, Suite L, 3475 Edison Way, Menlo Park, CA 94025 (US).

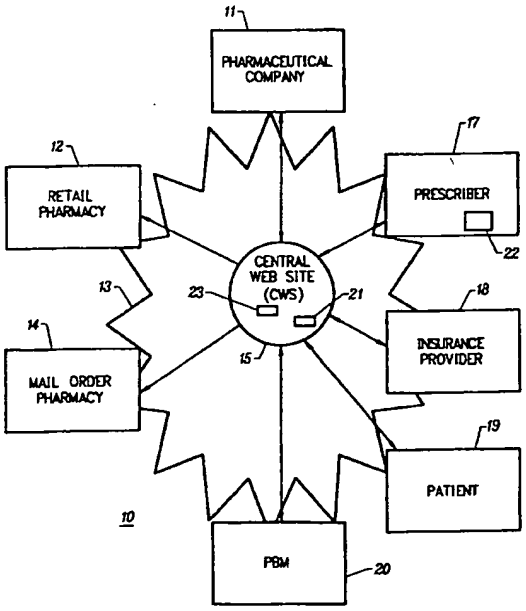
(81) Designated States *(national)*: AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, CA, CH, CN, CU, CZ, DE, DK, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MD, MG, MK, MN, MW, MX, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, UA, UG, UZ, VN, YU, ZW.

(84) Designated States *(regional)*: ARIPO patent (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GW, ML, MR, NE, SN, TD, TG).

Published:
— *With international search report.*
— *Before the expiration of the time limit for amending the claims and to be republished in the event of receipt of amendments.*

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

(54) Title: NETWORK-BASED INFORMATION MANAGEMENT SYSTEM FOR THE CREATION, PRODUCTION, FULFILLMENT, AND DELIVERY OF PRESCRIPTION MEDICATIONS AND OTHER COMPLEX PRODUCTS AND SERVICES



(57) Abstract: An information management system uses electronic transmission methods for the communication of prescription medications and confidential patient records over public or private networks while meeting the code requirements of Federal and State pharmaceutical and medical boards. The invention comprises methods of applying encryption and authentication methods; such as using asymmetric cryptographic algorithms (public-private key-pairs) or symmetric cryptographic algorithms (shared secret key) or any other encryption and authentication methods; and the prescribers' physical signature, to achieve the required levels of security, confidentiality, non-repudiation, and authentication. Such methods have security and authentication exceeding that of facsimile transmission, which has been commonly accepted and used for transmitting and fulfilling prescription medications in most States of the United States with participation of multiple parties and requiring high levels of security, authentication and nonrepudiation, such as prescription medications, and medical records. This invention is also applicable to the information management of other complex products and services with participation of multiple parties and requiring high levels of security, authentication and non-repudiation.

WO 01/09701 A1

Network-Based Information Management System for The Creation, Production, Fulfillment, and Delivery of Prescription Medications And Other Complex Products and Services

BACKGROUND OF THE INVENTION

TECHNICAL FIELD

The invention relates to information management systems. More particularly, the invention relates to a network based information management system for the creation, production, fulfillment, storage, processing, and delivery of complex products and services with participation of multiple parties and requiring high levels of security, authentication, confidentiality, and non-repudiation, such as prescription medications and medical records.

DESCRIPTION OF THE PRIOR ART

Significant advances are being made in the information technologies, including computing hardware platforms, local area networks (LANs), wide area networks (WANs), Internet connectivity, wireless communication, portable computing devices, powerful operating systems, user-friendly internet browsers and search engines, relational and object-oriented databases capable of efficiently handling large amount of data, advanced encryption protocols for secure communication of confidential information on public networks, and cost-effective and practical authentication and logging methods for secure transaction execution with acceptable tracking and non-repudiation

According to recent statistics from many health care and insurance organizations, healthcare is the largest single sector of the U.S. economy of approximately $ 1 trillion of annual spending, or over 14% of the nation's gross domestic product. Medication covers over 12 to 15% of the healthcare spending in the U.S.

Healthcare managed operations (HMOs) have recently made significant progress in containing the rapidly escalating costs of hospital, clinic, medical testing/diagnosis, and physician care. The processes for prescription medication creation and fulfillment continue to be fragmented and inefficient. The present workflow of the prescription medication creation and fulfillment has not benefited from any significant automation and process improvement. Presently, there are about 850,000 prescribers, including 650,000 physicians, writing over 2.5 billion prescriptions per year in the U.S.

In practice, the prescriber, after diagnosing the patient, manually writes a prescription on a paper pad, with a notation in the patient's medical chart, usually without complete access to the latest medical records of the patient from other medical organizations, or access to the relevant formulary and generic programs of the healthcare insurance provider, or access to the latest medication information from pharmaceutical manufacturers or healthcare research centers.

The patient then takes the written prescription to a retail pharmacy in the neighborhood for same day fulfillment. Retail pharmacies typically fill prescriptions for up to thirty days. The pharmacist enters the written prescription manually into the pharmacy computer and database system. A computer company provides an electronic connection between the pharmacy and the proper Pharmaceutical Benefit Manager (PBM) according to the patient insurance card, if the patient is insured.

At this point, the formulary and/or generic drug programs of the insurance provider may be displayed to the pharmacist. If the prescriber had not reviewed and selected from the formulary and/or generic drug programs, it is inefficient at this point to make changes in the prescription because the patient usually prefers to consult the physician/prescriber first, which is time consuming. The pharmacist may call the prescriber to change the prescription. However, to minimize waiting time, the patient in most cases ends up buying the prescribed medication at a higher co-payment. Because of such low compliance to formulary and generic programs, the cost of fulfilling the prescription is also higher for the insurance provider.

Once the prescription is fulfilled, the PBM takes responsibility for invoicing and collecting payment from the appropriate healthcare insurance companies, government, and/or employers and makes payments to the pharmacies on a monthly basis.

The patient or prescriber can also send the prescription by mail or fax to a mail order pharmacy for up to three months fulfillment. This approach results usually in a lower co-payment and is of less cost to the healthcare insurer. The mail order pharmacy must confirm the authenticity of the received prescription by calling the physician directly to meet the code and guidelines of the Federal and State pharmaceutical boards. The mail order pharmacist then follows the same steps as the retail pharmacist as described above with the same inefficiencies.

The code, laws, rules and regulations of the State and Federal pharmacy boards for the transmission of prescription medication are summarized below:

A medication prescription can be oral, written, or electronically transmitted. Electronic transmission of the prescription includes both images and data. An electronic image transmission prescription must comprise a facsimile of the prescription order that includes the physician's signature, name,

address, telephone number, license classification, and federal registry number (if a controlled substance is prescribed); the name and address of the patient; and the name and quantity of the drug, directions for use, and the date of issuance.

An electronic data transmission prescription comprises any prescription order, other than electronic image transmission prescription, that is electronically transmitted from a licensed prescriber to a pharmacy. This includes electronic, or e-mail on private or public networks.

For oral or electronic transmission, the pharmacist or furnisher must take appropriate steps to determine that the person who transmits and prescribes the prescription is authorized to do so. The pharmacist must record the name of the person who transfers the order. This does not apply to orders for Schedule II controlled substances, as they have considerably more stringent requirements.

For dangerous drugs, except for any Schedule II controlled substance, a written order of the prescriber that contains at least the name and address of the prescriber, name and address of patient, name and quantity of drug, direction of use, and date of issue may be treated as a prescription by the dispensing pharmacist, as long as additional information of the prescriber is readily retrievable in the pharmacy.

Facsimile copies of the prescriptions are acceptable as long as the pharmacist can call the prescriber, if needed, to authenticate and verify the information contained therein.

Facsimile transmission is considered secure because it is a point-to-point communication. However, transmitting prescriptions on public networks, such as the Internet, is not considered secure because it is difficult to ensure the authenticity of the prescriber and to maintain the confidentiality of

information in the prescription relating to the patient.

J. Edelson, C. Mayaud, *Prescription Creation System*, U.S. Patent No. 5,737,539 (7 April 1998) disclose an electronic prescription creation system for use by professional prescribers at the point of care which has a prescription division subsystem that permits creation of a single prescription which is automatically divided into two components for fulfillment of one portion quickly and locally at higher cost and of another portion by remote mail order, thereby taking more time but providing a cost saving for a major part of the prescription. Edelson *et al* do not address the issues of authentication and non-repudiation. Rather, they teach that "better security, in terms of ensuring that the filled prescription is released to the intended patient, or their agent, may be provided, by treating an electronic prescription transmission to a pharmacy as an advisory against which fulfillment may be initiated, wile the prescription is released only in exchange for a manually signed hard (paper) copy."

C. Mayaud, *Prescription Management System*, U.S. Patent No. 5,845,255 (1 December 1998) disclose an electronic prescription creation system. However,, Mayaud does not teach an electronic prescription delivery system that addresses the issues of security, authentication, and non-repudiation.

Other electronic prescription systems have suggested that a facsimile transmission may be used to provide an authenticated copy of a prescription. However, such facsimile transmissions comprises documents that are easy to forge. Accordingly, the pharmacist is compelled to telephone the prescriber and verify that the prescription was in fact written.

It would be advantageous to provide the confidentiality, authentication, and non-repudiation needed to meet the code requirements of Federal and State pharmaceutical and medical boards for the transmission of prescription medication and patient medical records using private or public

networks, such as the Internet, between all the parties involved, such as prescribers, physicians, patients, pharmacies, PBMs, third-party payers (insurance companies, employers, government), and pharmaceutical companies.

SUMMARY OF THE INVENTION

The invention provides a solution to the inefficiency problems attendant with the workflows associated with the manual creation and fulfillment of prescriptions for medication, and of the manual creation of confidential patient health information. The invention uses the latest network based information technologies, advanced encryption protocols for secure communication of confidential information on public networks, and cost effective and practical authentication and logging methods for secure transaction execution with acceptable tracking and non-repudiation.

The invention provides an information management system that uses electronic transmission methods for the communication of prescriptions for medication and confidential patient records and information over public networks while meeting the code requirements of Federal and State pharmaceutical and medical boards.

The invention applies various encryption and authentication methods, including asymmetric signature and encryption algorithms (those that use public-private key-pairs), symmetric encryption algorithms (using a shared secret key), cryptographic keyed and un-keyed one-way hash functions, and other, non-cryptographic means, such as the image of the prescriber's physical signature and/or images of other transaction participant's physical signature, to achieve the required levels of security, confidentiality, non-repudiation, and authentication. The images of the physical signatures are optionally used to provide a human-readable confirmation of the authentication of the digital signatures of electronically transmitted documents and messages. Thus, the code requirements of Federal and State

pharmaceutical boards can be met. Such methods have security, confidentiality, and authentication superior to facsimile transmission, which is accepted and commonly used now for transmitting and fulfilling prescriptions for medication in most States (over 39 States presently) of the United States. Facsimile transmission is considered secure because it is a point-to-point communication, and is acceptable as long as the pharmacist can telephone the prescriber, if needed, to authenticate and verify the information contained therein.

Such capabilities enable new information management systems to automate and improve the efficiency of the work flows for the creation and fulfillment of prescriptions for medication and for healthcare information; and the interaction between prescribers, patients, pharmacies, PBMs (Pharmaceutical Benefit Managers), and pharmaceutical companies, with the following benefits:

- Physicians and other prescribers, who are the decision-makers with regard to the prescription of medication, can prescribe and send prescriptions to pharmacists more efficiently and with more awareness into the patient's complete medical history. The invention also provides the latest information concerning prescription medication from stored medical history databases, including other physicians' medical treatment as well as relevant formulary, generic, and compliance programs of third party payers.

- Patients have more efficient and convenient dispensing of medication either from mail order or retail pharmacy, in a transparent way, e.g. where the prescription is electronically transmitted directly from the physician's office without logistics of faxing, mailing, telephone call delays, or delays in mail order medication delivery. An immediate short-term supply of the prescribed medication can be obtained from physician's samples or from a local retail pharmacy. The electronic prescription can also be electronically transmitted to a retail pharmacy directly and the

patient can pick up the prescribed medication the same day for use until the mail order delivery of the rest of the prescription is received. Patients can also save money by using a mail order pharmacy.

- Pharmacies can fulfill prescriptions more efficiently from the electronically transmitted data. Automated integration of the prescribing and fulfillment systems dramatically reduces the likelihood of transcription errors by the pharmacist, decreases the cost, and improves the efficiency of prescription fulfillment.

- Third party payers, *e.g.* insurance companies, government agencies, and employers, also save money because this invention provides a more transparent use of mail order and prospective management of higher formulary and higher generic compliance.

- In addition more complete medical information is available to those making healthcare decisions at the point of care, resulting in more efficient and higher quality medical treatment.

BRIEF DESCRIPTION OF THE DRAWINGS

Fig. 1 is a block schematic diagram showing an information management system for the preferred embodiment of the prescription medication system and illustrates the logical relationships and the information communication across a network between the key entities during a prescription creation and fulfillment process;

Fig. 2 is a flow chart showing the creation and fulfillment of a prescription for medication in the information management system shown on Fig. 1;

Fig. 3 is a flow diagram showing a process for sending and receiving prescriptions for medication to achieve the security, authentication,

and non-repudiation that is necessary to satisfy the code requirements of Federal and State pharmaceutical and medical boards in accordance with the invention.

Fig. 4 is a flow diagram showing the general system configuration and hierarchical levels of authentication in accordance with the invention;

Fig. 5 details system access controls and required authentication levels. where all authentication levels can use two-factors except for application managers in accordance with the invention; and

Fig. 6 is a flow diagram showing a presently preferred procedure employed in meeting the code requirements of Federal and State pharmaceutical and medical boards in accordance with the invention.

DETAILED DESCRIPTION OF THE INVENTION

This invention relates to the application of leading-edge network-based information technologies and recent advances of encryption and digital signature schemes to the creation of specifications, and to the development, production, fulfillment, delivery, and management of complex products and services which require:

- Detailed latest versions of products and services information, and/or
- Historical customer/product/services information, and/or
- Latest and current contract information, and/or
- Latest options for production and delivery alternatives, and/or
- From multiple, extensive, diverse, or remote information

sources, and/or

- With high requirements of information-security, and/or source authentication, and/or transaction tracking/logging/security/non-repudiation.

The herein disclosed application of leading edge network based information technologies results in more efficient, economic, and accurate creation, implementation, and delivery of complex products and services for the sources and parties involved.

Examples of such products and services which benefit from applications of the herein-described invention include:

- Creation of prescriptions and the delivery of medication;
- Diagnosis and solution of equipment malfunctioning where sensitive and confidential information is involved;
- Ordering and communication of results for medical laboratory tests, radiation tests, and remedies;
- Patient medical records;
- Diagnosis, testing, and remedy of diseases;
- Ordering of restricted products and services with complex contract requirements and/or Federal/State restrictions, such as firearms, and hazardous materials; and
- Ordering of agricultural/veterinary supplies and

materials.

The preferred embodiment of the invention, described in more detail below, is for a medication prescription and healthcare management system to create a more automated workflow, which provides:

- More efficient prescribing of medication by physicians and prescribers, and higher quality of patient care with more available data on patient medical history;

- Latest medication information from pharmaceutical companies and research sources; and most recent patient insurance coverage information, including formulary and generic compliance programs;

- More efficient and cost effective fulfillment of medication by the pharmacist, better cost saving for health care insurance companies from better results of formulary, generic, mail-order for maintenance drugs, and patient compliance programs;

- Secure storage and convenient retrieval of more complete medical and health information at the point of care, resulting in higher quality of health care; and

- More efficient prescription fulfillment through retail and mail order channels with lower cost for the patients, resulting from the integration of the electronic prescribing, transmission, and fulfillment systems.

It should be clear to those skilled in the art how to implement the preferred embodiment of the invention from the disclosure herein and to provide other applications and workflow in accordance with the invention herein.

Fig. 1 is a block schematic diagram of an information management system for the presently preferred embodiment of a medication prescription system 10, illustrating the logical relationships and the communication of information across a network 13 between key entities of the invention during a prescription creation and fulfillment process.

A central server (CS) 15 is accessible through a network 13, such as the Internet, *e.g.* the World Wide Web, or any other private or public network, from each authorized prescriber's office 17 via an access device 22, such as a computer terminal, a PC connected with a modem, or a portable hand-held device. The network 13 may have any logical or physical configuration as long as each key entity has communication access to the CS. The CS registers and issues unique cryptographic keys for each qualified prescriber. These cryptographic keys may be either asymmetric keys (pair of public and private digital encryption keys used with an asymmetric cryptographic algorithm), or symmetric keys (shared secret digital encryption keys used with a symmetric cryptographic algorithm or with a keyed one-way hash function). The CS stores these keys and the registration information in a secure database 21 at the CS. The registration for each prescriber includes all the relevant and necessary information, such as name, address, qualification, drug registration number, and signature image, and may also include a mechanism for performing frequent verification of the validity of the drug registration number. Each prescriber has access to their aforementioned unique cryptographic key via a privately selected user name/password scheme or other commonly known authenticated access scheme (such as signature recognition or other biometric authentication scheme including finger-prints, eye-retina scans, or voice recognition).

In the presently preferred embodiment of the invention, the CS also registers and issues unique cryptographic keys similar to those mentioned above for each participating retail pharmacy 12 and mail order pharmacy 14. The CS also keeps in its secure database the aforementioned unique

cryptographic keys and the registration information including all the necessary and relevant information about the qualification and registration of the pharmacy.

The CS also creates a private database 23 for each patient 19, including personal information, healthcare insurance coverage, and relevant medical/drug historical information. The patient database is a virtual medical record (VMR) which grows with time. The patient database is protected by controlled secure access, such that its contents are only available to healthcare providers, prescribers, pharmacists, insurance providers, and the patient, with proper security code as authorized by the patient.

The CS has access to the participating PBMs 20, including access to all of the latest information on the insurance coverage of the patients, and on relevant formulary and generic programs. The CS has also access to the latest medication and drug information from the pharmaceutical manufacturers and healthcare research and information centers.

Additional access to the CS in the presently preferred embodiment of the invention may also include any of the following:

- Patients 19 may have the option to participate in the secured access to the CS by registering and having assigned unique cryptographic keys, analogous to those mentioned above, for controlled access to their medical records, for inquiry on status of prescription fulfillment, reorder of prescribed medication, and/or information about latest medication, diseases, and medical treatments.

- Healthcare insurance providers 18 may have the option to participate in the secured controlled access to the CS by registering with the CS and having assigned unique cryptographic keys, analogous to those mentioned above, for controlled access to the medical records of their

covered patients for coverage approval purposes, data collection or any other approved purposes.

- Pharmaceutical manufacturers 11 may also have the option to participate in selected secured controlled access to the CS by registering and having the CS assign unique cryptographic keys, analogous to those mentioned above, for controlled access to statistical medical or medication usage information, without violating the privacy and security of patient records.

The availability of all the above described information in a secure and scalable database, along with the controlled, secured, authenticated, and highly available access to all the various sources and parties involved in the prescription and medical records creation and fulfillment process, allows the invention to provide higher efficiency, lower cost, and more convenience for all the parties.

Fig. 2 is a flow chart showing a process for the creation and fulfillment of a prescription for medication in accordance with the information management system shown in Fig. 1. According to this embodiment of the invention, the following workflow for the creation and fulfillment of a prescription for medication occurs:

The prescriber makes a diagnosis of the patient(100) and is ready to prescribe the proper medication.

To select the proper prescription medication, the prescriber accesses the CS (102) using a computer terminal or portable device in the prescriber's office or with any other suitable electronic device, and brings up the patient VMR, insurance coverage information, and formulary and generic programs, as well as the latest information on medication from pharmaceutical companies and research centers.

The prescriber examines the patient's relevant medical history and any relevant formulary, generic, and compliance programs (104). For a new patient, all the new relevant medical, personnel, and insurance coverage information of the patient can be entered in the CS by the prescriber or his/her assistant, so that it will not have to be re-entered again by other participants.

The prescriber enters the diagnosis of the patient and can review the latest available information about all the relevant medications from the pharmaceutical manufacturers and medical research centers related to this diagnosis. The prescriber also can review any relevant formulary, generic, and compliance programs. The prescriber selects and enters the optimum prescription medication (106) according to all the available data, including the patient information, diagnosis, condition, treatment objectives, medication name and dosage, and treatment directions and details.

The patient selects (108) either a local retail pharmacy, a mail order pharmacy, or both, for the fulfillment of the prescription for medication. The retail pharmacy is convenient for less than a thirty-day supply presently, and same day fulfillment. The mail order pharmacy is more convenient for maintenance and chronic medication as it provides a ninety-day supply with less co-payment, a lower prescription price, and more convenient mail order refill. The patient may select a portion of the prescription to be fulfilled from a retail pharmacy for immediate use for few days until the rest of the prescription is fulfilled by the mail order pharmacy at lower cost. The patient may also use a short-term supply of prescription medication provided by prescriber's samples until the mail order medication is received.

The prescriber transmits electronically the prescription for medication to the CS, secured using encryption and digital signature schemes disclosed below (110).

The CS decrypts and electronically authenticates the received electronic

prescription for medication (112). Such decryption and authentication can be done automatically, and without the need of manual intervention. The CS transmits electronically the prescription to the selected retail and/or mail order pharmacy using the encryption and digital signature schemes disclosed below (114) in connection with Fig. 6.

The retail and/or the mail order pharmacy receives the electronically transmitted prescription (116; 138) and feeds the prescription electronic information directly into an electronic software system. . This can be done automatically and without the need for manual intervention.

Decryption and authentication of the prescription medication received from the CS at the retail pharmacy and/or mail order pharmacy can be performed automatically (118; 140). The prescription and the authentication confirmation, and an optional image signature of the prescriber (either stored at the CS or electronically transmitted), are stored in an electronic secure database and/or in printed formats.

The retail and/or mail order pharmacy fulfills the prescription (120; 142) from the electronic data received. This can be done automatically without manual intervention, and without the need to make adjustments for compliance with formulary and generic programs, and without the need to call the prescriber for confirmation and authentication. This results in significant efficiency improvement in operation.

The retail and/or mail order pharmacy delivers the medication to the patient and collects the payment from the patient, PBMs, and/or insurance companies using commonly accepted collection practices (122; 144).

The patient can access the CS (124) for medical information about the medication, diseases, or for tracking the status of the prescription. The patient can also order refills of the prescription by electronic

transmission to the CS. Proper priority for secure access is given to different users and participants of the system.

The CS confirms the refill request (126) with the prescriber by electronic transmission with similar encryption and authentication methods as described below.

The CS electronically transmits the confirmed and authenticated refill prescription to the selected retail and/or mail order pharmacy (128) and updates the VMR.

Following the same procedure disclosed above, the selected retail and/or mail order pharmacy refills the prescription (130; 132).

Following the same procedure disclosed above, the refilled prescription is delivered to the patient (136; 134) and the payment is collected from patient, PBMs, and/or insurance companies using commonly accepted collection practices.

Fig. 3 is a flow diagram which shows the application of encryption and authentication methods (such as the use of asymmetric public-private key pair algorithms, symmetric shared secret key algorithms, or any other encryption and authentication methods), with an optional prescriber's physical signature, to achieve the required security, confidentiality, non-repudiation, and authentication that is necessary to satisfy the code requirements of Federal and State pharmaceutical and medical boards.

Fig. 3 illustrates secure electronic transmission of the prescription from the prescriber to the CS, and then from the CS to the dispensing pharmacy. The prescription is encoded (300) using a standardized format that can be electronically transmitted through the network and automatically processed by the prescriber, CS, and dispensing pharmacy. The encoded prescription

is digitally signed by the prescriber (300). The signed, encoded prescription is encrypted for transmission over the network (310). The CS receives and decrypts the prescription, authenticates the prescriber signature, adds its digital signature to the prescription, if need be, and otherwise prepares the prescription for transmission to the selected pharmacy (320). The CS next encrypts the prescription, with its attached digital signatures, for transmission over the network (330). The pharmacy receives and decrypts the transmission, authenticates the prescriber, and fulfills the prescription by dispensing the medication to the patient (340).

Fig. 4 illustrates an example implementation of a CS showing methods of security, access control, availability, and reliability. The CS 400 is implemented using one or more software applications, running on one or more hardware server platforms, in a controlled access, physically secure environment. In the preferred embodiment of the invention, system administrators 401 who are authorized physical access to the hardware to perform routine functions, including system maintenance, backup, and monitoring, are required to use strong, two-factor authentication 402 involving a password and one other method, such as possession of a physical token or biometric verification. Application managers 403 authorized to maintain access controls for participants to applications and data, or to access databases containing sensitive information, are required to use an additional authentication factor over and above that required by system administrators.

The CS implements security policies designed to protect the privacy and safeguard the confidentiality of sensitive information entrusted to it. Examples of such information include patient records and participant business practices. These policies are enforced using a combination of data encryption and operating system and database access controls 411. Participants who access the CS, including patients 404, clinics 405, payment centers 406, pharmacies 407, research centers 408, insurance companies 409, and hospitals 410, are required to authenticate themselves using, at a

minimum, an appropriate password transferred over a secure, encrypted communications channel. In some cases, additional authentication factors are used. The CS itself uses a method such as a public key digital signature to authenticate itself to participants and establish the secure, encrypted communications channel.

Fig. 5 illustrates the physical and logical security policies for application 501 and database 502 servers, and for the database image itself 503. Server computers are physically protected within a controlled environment 500 requiring proper (*e.g.* two-factor) authentication for physical access. All such access is logged. To stop potential attacks on the server and the applications it runs from unidentified sources on the network 505, a firewall 504 is used to provide a logical perimeter. Both packet filtering and application level filtering can be used. Mirroring of the database 503 can be performed for reliable operation.

The procedure employed in the preferred embodiment of the invention applying encryption and authentication schemes for meeting the code requirements of Federal and State pharmaceutical and medical boards described above is as follows (see Fig. 6):

The CS receives an encrypted prescription, and the digital signatures that are necessary to authenticate the prescription, and then sends them to the selected mail order or retail pharmacy.

1. Each participating prescriber and pharmacy is assigned a unique cryptographic key, such as asymmetric private-public key-pair, symmetric shared secret key, or any encryption scheme. (600).

2. An option to provide humanly readable verification of authentication is to use the digitized signature image of the prescriber and store it at the prescriber's computer and/or at the CS central

office in secure data storage (602).

3. A digital signature can be made with various well-known schemes, such as by encrypting a hash code (or message digest) of the original prescription using the prescriber's asymmetric private key, or creating a message digest using the prescriber's symmetric shared secret key and a suitable keyed hash algorithm. The prescriber's digital signature is electronically transmitted to the CS (604).

4. The prescription for medication, along with a time stamp, and an optional image of the prescriber's signature, is encrypted and transmitted electronically to the CS (606). The encryption method can employ one of a variety of schemes consistent with practice of the art, including use of a standard security protocol (*e.g.* Secure Sockets Layer, or SSL).

Note: Steps 3 and 4 above can be transmitted together or they can be transmitted separately.

5. At the CS, the message containing the prescription is decrypted to obtain the original, plaintext prescription. (608).

6. Authentication of the prescriber digital signature in the case of the use of an asymmetric public key encryption algorithm is accomplished by first computing the hash code over the decrypted received prescription (610). In the case of a symmetric key algorithm, the keyed hash is computed using the shared secret key.

7. Next, the received digital signature is decrypted using the prescriber's asymmetric public key or the prescriber's symmetric shared secret key. (612).

8. Next, the successful comparison between the hash code computed over the received decrypted prescription (from Step 6 above) with the hash code decrypted in the received digital signature (from Step 7 above) provides the required digital signature or proof-or-origin authentication of the prescriber (614). An optional confirmation of the reception, successful decryption and authentication of the prescription may be sent by the CS to the prescriber electronically, encrypted and authenticated using methods such as those outlined above.

9. With the digital authentication of the prescriber, the image of the prescriber's signature from either the CS database or from the decrypted transmitted prescription is optionally placed on the prescription, thereby providing an electronic image that is identical to that of a facsimile transmission, and is humanly readable. The electronic and hard copies are filed with the CS and/or with the selected pharmacy dispensing the medication (616). This step provides authentication that meets and exceeds the code requirement of the majority of State and Federal pharmaceutical boards equivalent to the facsimile transmission.

10. The CS can provide its own digital signature over the authenticated prescription, including with it the prescriber name and all relevant information, using a digital signature scheme such as one described above.. This digital signature is electronically transmitted to the selected retail and/or mail order pharmacy (618).

11. The CS sends the request of the prescription with a time stamp over the network to the selected mail order or retail pharmacy, encrypted and authenticated using methods similar to those outlined above (6420).

12. The selected pharmacy decrypts the prescription , which, once in plaintext form, can be printed with the image of the prescriber's signature, after completing the authentication of the CS in Step 13 below (622).

13. Authentication of the digital signature from the CS can be performed according to the digital signature at the CS, as in Steps 6, 7, and 8 above (624). The mail order and/or retail pharmacy has the option to perform this digital authentication automatically without the need of manual intervention.

14. After confirming the authentication of the digital signature of the CS, the mail order and/or retail pharmacy dispenses the medication by mail or directly to patient (as requested) (626). An optional confirmation of the successful reception, decryption, authentication, and fulfillment of the prescription is electronically sent to the CS, and in turn optionally sent to the prescriber for archiving and non-repudiation purposes.

Notice that the prescription printed at the dispensing pharmacy and the CS can optionally include the image of the prescriber's signature from either the stored image in the secured database of the CS or the transmitted image from the prescriber's computer. The pharmacy and/or the CS can store for the prescription and the confirmation of fulfillment the printed copy of in their files, and/or the electronic image in their computer memory database, for up to seven years or longer as required.

Although the invention is described herein with reference to the preferred embodiment, one skilled in the art will readily appreciate that other implementations and other applications may be substituted for those set forth herein without departing from the spirit and scope of the present

invention. Accordingly, the invention should only be limited by the Claims included below.

CLAIMS

1. A system for the creation, development, production, fulfillment, delivery, and management of complex products and services, comprising:

a central site or server (CS) accessible through a network to each of at least one subscriber via an access device;

said CS comprising means for issuing unique cryptographic keys for each of at least one subscriber ; and

a secure database for storing said issued cryptographic keys wherein each at least one subscriber has access to its said issued unique cryptographic keys via an authenticated access scheme.

2. The system of Claim 1, wherein each at least one subscriber has access to its said issued unique encryption keys via any of a privately selected user name/password scheme, and/or a signature, finger-print, eye-retina, or biometric recognition scheme.

3. The system of Claim 1, wherein said secure database containing a signature image of said at least one subscriber.

4. The system of Claim 1, wherein said CS comprises:
means for issuing asymmetric cryptographic public-private key pair for said at least one subscriber.

5. The system of Claim 1, wherein said CS comprises:
means for issuing symmetric cryptographic key for said at least one subscriber.

6. The system of Claim 1, wherein transmission of messages is between said at least one subscriber having access through said network and

said CS, using said cryptographic means to achieve confidentiality, authentication, and non-repudiation of said transmission of messages.

7. The system of Claim 1, wherein transmission of messages is between said at least on subscriber having access through said network and said CS, using said issued unique cryptographic keys for security, and digital signatures and said at least one subscriber' signature image to achieve confidentiality, humanly readable authentication, and non-repudiation of said transmission of messages.

8. The system of Claim 1, wherein said secure database stores said at least one subscriber's name, address, necessary qualification, and relevant information.

9. The system of Claim 1, wherein said CS supports the creation of prescriptions and delivery of medication.

10. The system of Claim 1, wherein said CS issues cryptographic keys to at least one authorized prescriber; and
wherein said CS keeps in its said secure database said at least one prescriber's name, address, all necessary qualification and relevant information.

11. The system of Claim 1, wherein said database stores a drug registration number.

12. The system of Claim 1, further comprising:
a mechanism for performing frequent verification of the validity of said drug registration number.

13. The system of Claim 12, wherein said verification is performed

automatically.

14. The system of Claim 1, wherein said CS supports the diagnosis and solution of equipment malfunctioning where sensitive and confidential information is involved.

15. The system of Claim 1, wherein said CS supports the diagnosis, testing, and remedy of diseases.

16. The system of Claim 1, wherein said CWS supports the ordering of restricted products and services with complex contract requirements and/or Federal/State restrictions.

17. The system of Claim 1, wherein said CS issues cryptographic keys to at least one participating pharmacy; and
wherein said CS keeps in its secure database all necessary and relevant information about the qualification and registration of said pharmacy.

18. The system of Claim 1, wherein said CS creates a private database for at least one patient, said private database including personnel information, healthcare insurance coverage, and relevant medical/drug historical information.

19. The system of Claim 18, wherein said private database is a virtual medical record (VMR) which grows with time.

20. The system of Claim 18, wherein said private database is protected by controlled secure access, such that its contents are only available to individuals and organizations as authorized by said patient.

21. The system of Claim 1, wherein said CS accesses at least one participating pharmaceutical benefit manager (PBM).

22. A system for the development, production, fulfillment, delivery, and management of complex products and services, comprising:

a central server (CS) accessible through a network to each of at least one prescriber via an access device, wherein said CS supports the creation of prescriptions and delivery of medication;

said CS comprising means for issuing unique encryption keys for each of at least one prescriber, wherein each prescriber has access to its issued unique cryptographic key via any of a privately selected user name/password scheme, a signature, finger-print, eye-retina, or biometric recognition scheme; and

a secure database for storing said cryptographic keys, wherein said secure database stores said prescriber's name, address, and qualification, wherein said database stores a drug registration number, wherein said CS creates a private database for at least one patient, said private database including personnel information, healthcare insurance coverage, and relevant medical/drug historical information, wherein said private database is protected by controlled secure access, such that its contents are only available to individuals and organizations as authorized by said patient;

wherein each said at least one prescriber has access to said issued unique cryptographic key via an authenticated access scheme; and

wherein said CS issues unique encryption keys to at least one participating pharmacy; and wherein said CS keeps in its secure database all necessary and relevant information about the qualification and registration of said at least one pharmacy

23. The system of Claim 22, wherein patients have secured access to said CS by using issued cryptographic keys for controlled access to their medical records, for inquiry on status of prescription fulfillment, reorder of prescribed medication, and/or information about latest medication, diseases, and medical treatments.

24. The system of Claim 22, wherein said database containing each prescriber's signature image,

25. The system of Claim 22, wherein said CS comprising means for issuing asymmetric cryptographic public-private key pair for said at least one prescriber.

26. The system of claim 22, wherein said CS comprising means for issuing symmetric cryptographic key for said at least one prescriber.

27. The system of Claim 22, wherein said CS accesses at least one participating pharmaceutical benefits manager (PBM).

28. The system of Claim 22, wherein healthcare insurance providers have secured controlled access to said CS by using issued unique cryptographic keys for controlled access to medical records of covered patients for coverage approval purposes or other approval purposes.

29. The system of Claim 22, wherein pharmaceutical manufacturers have secured controlled access to said CS by using issued unique cryptographic keys for controlled access to statistical medical or medication usage information, without violating the privacy and security of patient records.

30. A process for the creation and fulfillment of a prescription for medication, comprising the steps of:

accessing a central server (CS) through a network from an authorized prescriber's office via an access device;

said prescriber selecting and entering a prescription medication;

selecting a pharmacy for fulfillment of said prescription; and

sending a first electronic transmission comprising said prescription to said CS using an encryption scheme;

wherein said CS decrypts and authenticates said first

electronic transmission of prescription received from said prescriber, and sending a second electronic transmission comprising said prescription to said pharmacy using an encryption scheme;

said pharmacy receiving said second electronic transmission and entering said prescription into an electronic system;

wherein said pharmacy decrypts and authenticates said second electronic transmission of prescription received from said CS; and

wherein said pharmacy fulfills said prescription from electronic data received in said second electronic transmission .

31. The process of Claim 30, further comprising the step of:

providing said patient's relevant medical history and any relevant formulary and generic compliance programs to said prescriber.

32. The process of Claim 30, wherein all the relevant medical, personnel, and insurance coverage information of the patient can be entered in said CS by said prescriber.

33. The process of Claim 30, further comprising the step of:

providing information about substantially all relevant medications from pharmaceutical manufacturers and/or medical research centers.

34. The process of Claim 30, wherein said patient may select a portion of said prescription to be fulfilled from a retail pharmacy and a portion of said prescription to be fulfilled by a mail order pharmacy.

35. The process of Claim 30, wherein said prescription, an authentication confirmation, and an optional image signature of said prescriber, are stored in a secure database by said CS or said pharmacy.

36. The process of Claim 30, wherein said pharmacy delivers said medication to said patient and collects payment from any of said

patient, at least one PBM, or at least one insurance company.

37. The process of Claim 30, wherein said patient orders refills of said prescription by sending an electronic transmission to said CS;

wherein said CS confirms said refill request with said prescriber by electronic transmission; and

wherein said CS electronically transmits said confirmed and authenticated refill prescription to said pharmacy.

38. A process for the creation and fulfillment of a prescription for medication, in which a prescriber accesses a central server (CS) through a network from an authorized prescriber's office via an access device; said prescriber selects and enters a prescription medication; a pharmacy for fulfillment of said prescription is selected; and said prescriber sends said prescription by electronic transmission, wherein said prescription is encrypted and digitally signed before it is sent over said network, said process comprising the steps of:

said CS receiving said prescription;

said CS decrypting said prescription;

said CS authenticating said prescription; and

said CS re-signing digitally and re-encrypting said prescription;

wherein said encrypted, authenticated prescription is sent over said network by said CS to said pharmacy.

39. The process of Claim 38, further comprising the step of:

recording said prescription for document retention purposes.

40. The process of Claim 38, wherein said pharmacy receives, decrypts, authenticates and fulfills said authenticated prescription and dispenses said prescribed medication to a patient.

41. The process of Claim 38, wherein said CS receives an

encrypted prescription and digital signatures that are necessary to authenticate said prescription and then sends them to said pharmacy.

42. The process of Claim 38, wherein said prescriber and said pharmacy are assigned unique cryptographic keys by said CS.

43. The process of Claim 38, wherein a signature image of said prescriber is digitized and stored at said prescriber's computer and/or at said CS in secure data storage.

44. The process of Claim 38, wherein said prescription, along with a time stamp, and an optional image of said prescriber's signature, is encrypted with an encryption key and electronically transmitted to said CS.

45. The process of Claim 38, wherein a digital signature is made by computing a hash code or cryptographically strong digest of said prescription, and encrypting said hash code with a prescriber's unique cryptographic keys, wherein said prescriber's digital signature is electronically transmitted to said CS.

46. The process of Claim 38, wherein said prescription, along with a time stamp, and an optional image of said prescriber's signature, is encrypted using an encryption key, and wherein a proof of origin authenticator is made by computing a keyed hash code of said prescription, and including said prescriber's unique cryptographic key in the computation of the keyed hash, wherein said prescription and said prescriber's authenticator are electronically transmitted to said CS.

47. The process of Claim 38, wherein said CS uses said cryptographic key to decrypt said encrypted prescription.

48. The process of Claim 47, wherein authentication of said

prescriber is accomplished using a digital signature comprising the successful comparison of a one-way hash, computed using an agreed upon hash function, over said decrypted prescription with a hash value obtained by decrypting said digital signature using a public key known to correspond to a private key used by said prescriber to sign said prescription.

49. The process of Claim 47, wherein authentication of said prescriber digital signature is accomplished using a cryptographic keyed hash function, where said cryptographic keyed hash function comprises a successful comparison of a one-way hash, computed using an agreed upon hash function and a shared secret value known only to said prescriber and a verifier, over said decrypted prescription.

50. The process of Claim 38, wherein an image of said prescriber's signature from either a CS database or from a decrypted transmitted prescription is placed on said prescription;
wherein authentication that meets code requirements of the State and Federal pharmaceutical boards equivalent to a facsimile transmission is provided.

51. The process of Claim 38, wherein said CS sends a confirmation of said prescription over said network to said pharmacy, wherein said confirmation is optionally encrypted with the cryptographic key and optionally includes a signature image of said prescriber.

52. The process of Claim 38, wherein a digital signature of said CS is made by computing said hash code over said authenticated prescription, including said prescriber's name, and then encrypting said hash code with either said pharmacy's unique symmetric encryption key or said CS 's unique private asymmetric encryption key;
wherein said digital signature is electronically transmitted to said pharmacy.

53. The process of Claim 38, wherein said pharmacy decrypts said

prescription with said cryptographic key and can optionally print said prescription with an image of said prescriber's signature.

54. The process of Claim 38, wherein authentication is performed by combining said decrypted received prescription from said CS according to claim 41 with a hash code and encrypting it with either said pharmacy's unique symmetric encryption key or said CS's unique public encryption key; wherein a successful comparison with a received digital signature from said CS provides digital authentication.

55. The process of Claim 38, wherein said digital authentication is performed automatically, and without manual intervention.

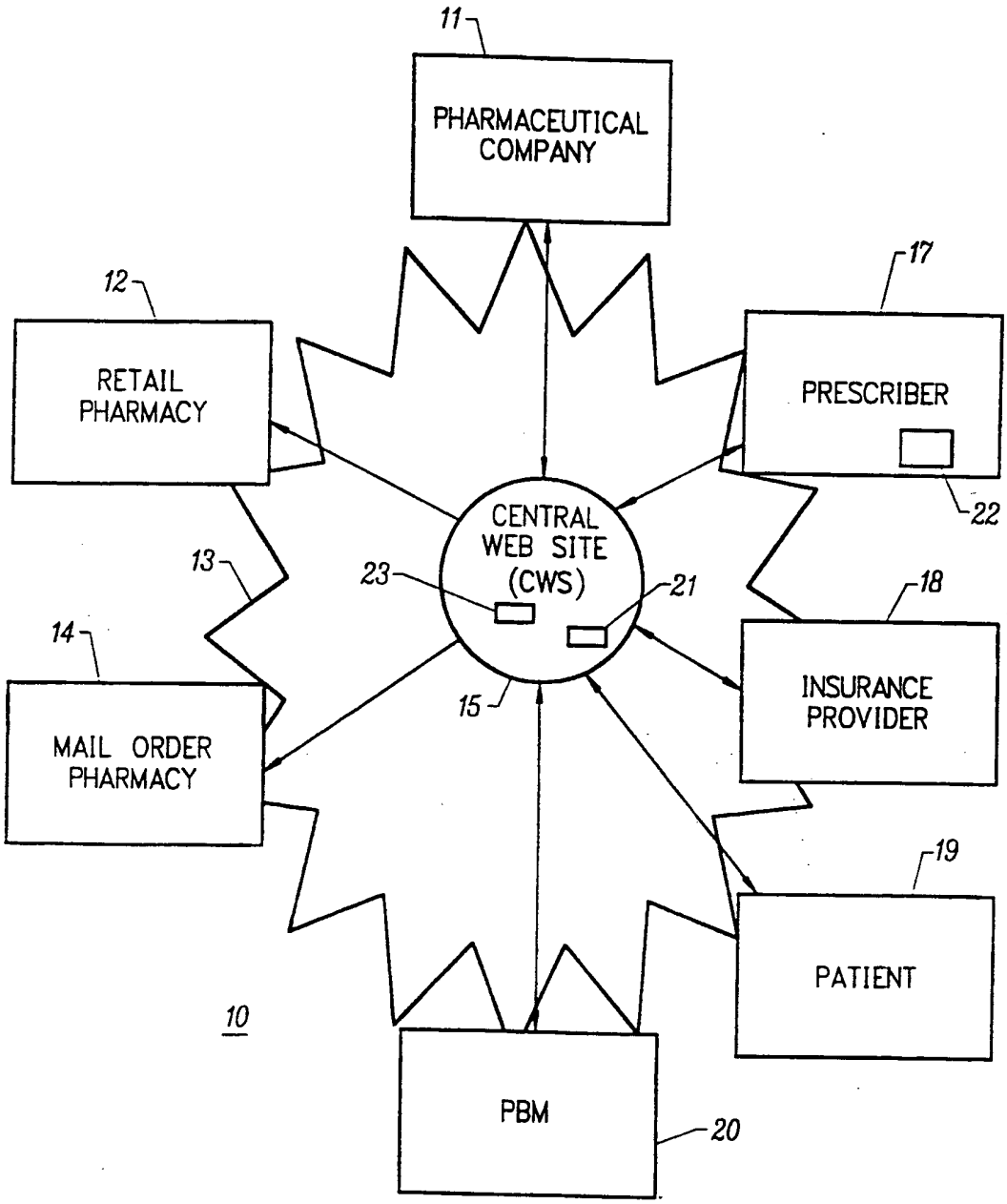

11
PHARMACEUTICAL COMPANY
12
RETAIL PHARMACY
17
PRESCRIBER
22
CENTRAL WEB SITE (CWS)
23
21
13
18
14
INSURANCE PROVIDER
15
MAIL ORDER PHARMACY
19
PATIENT
10
PBM
20

FIG. 1

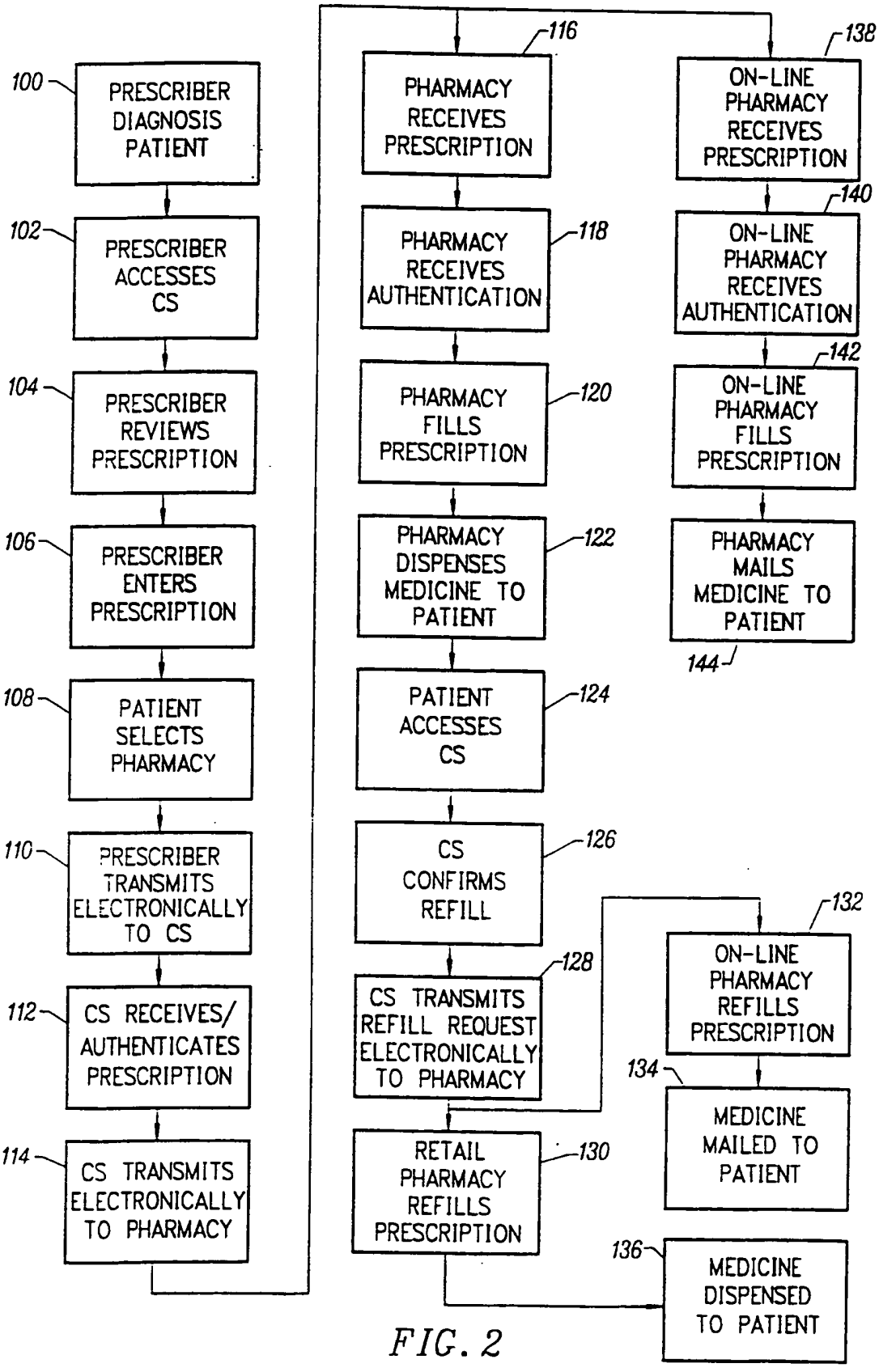

100
PRESCRIBER DIAGNOSIS PATIENT
102
PRESCRIBER ACCESSES CS
104
PRESCRIBER REVIEWS PRESCRIPTION
106
PRESCRIBER ENTERS PRESCRIPTION
108
PATIENT SELECTS PHARMACY
110
PRESCRIBER TRANSMITS ELECTRONICALLY TO CS
112
CS RECEIVES/ AUTHENTICATES PRESCRIPTION
114
CS TRANSMITS ELECTRONICALLY TO PHARMACY
116
PHARMACY RECEIVES PRESCRIPTION
118
PHARMACY RECEIVES AUTHENTICATION
120
PHARMACY FILLS PRESCRIPTION
122
PHARMACY DISPENSES MEDICINE TO PATIENT
124
PATIENT ACCESSES CS
126
CS CONFIRMS REFILL
128
CS TRANSMITS REFILL REQUEST ELECTRONICALLY TO PHARMACY
130
RETAIL PHARMACY REFILLS PRESCRIPTION
132
ON-LINE PHARMACY REFILLS PRESCRIPTION
134
MEDICINE MAILED TO PATIENT
136
MEDICINE DISPENSED TO PATIENT
138
ON-LINE PHARMACY RECEIVES PRESCRIPTION
140
ON-LINE PHARMACY RECEIVES AUTHENTICATION
142
ON-LINE PHARMACY FILLS PRESCRIPTION
144
PHARMACY MAILS MEDICINE TO PATIENT

FIG. 2

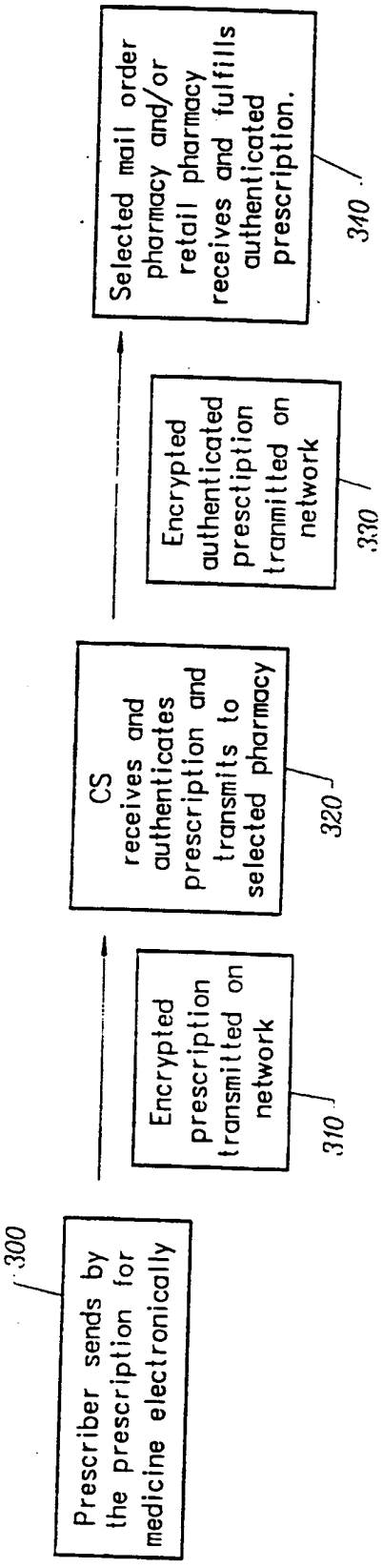

Prescriber sends by the prescription for medicine electronically
300
Encrypted prescription transmitted on network
310
CS receives and authenticates prescription and transmits to selected pharmacy
320
Encrypted authenticated prescription tranmitted on network
330
Selected mail order pharmacy and/or retail pharmacy receives and fulfills authenticated prescription.
340

FIG. 3

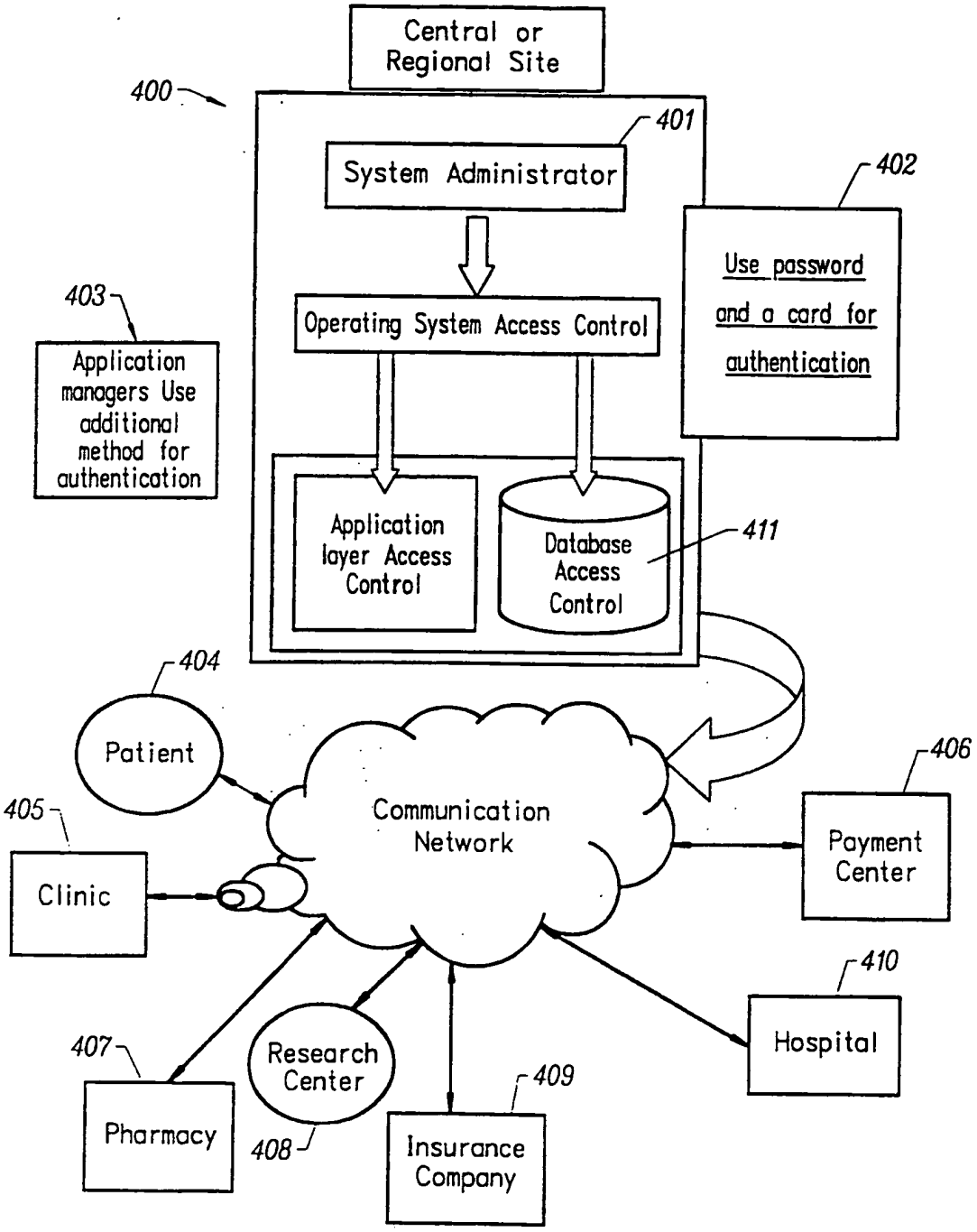

Central or Regional Site
400
401
System Administrator
402
Use password and a card for authentication
403
Application managers Use additional method for authentication
Operating System Access Control
Application layer Access Control
Database Access Control
411
404
Patient
405
Clinic
Communication Network
406
Payment Center
410
Hospital
407
Pharmacy
Research Center
408
409
Insurance Company

FIG. 4

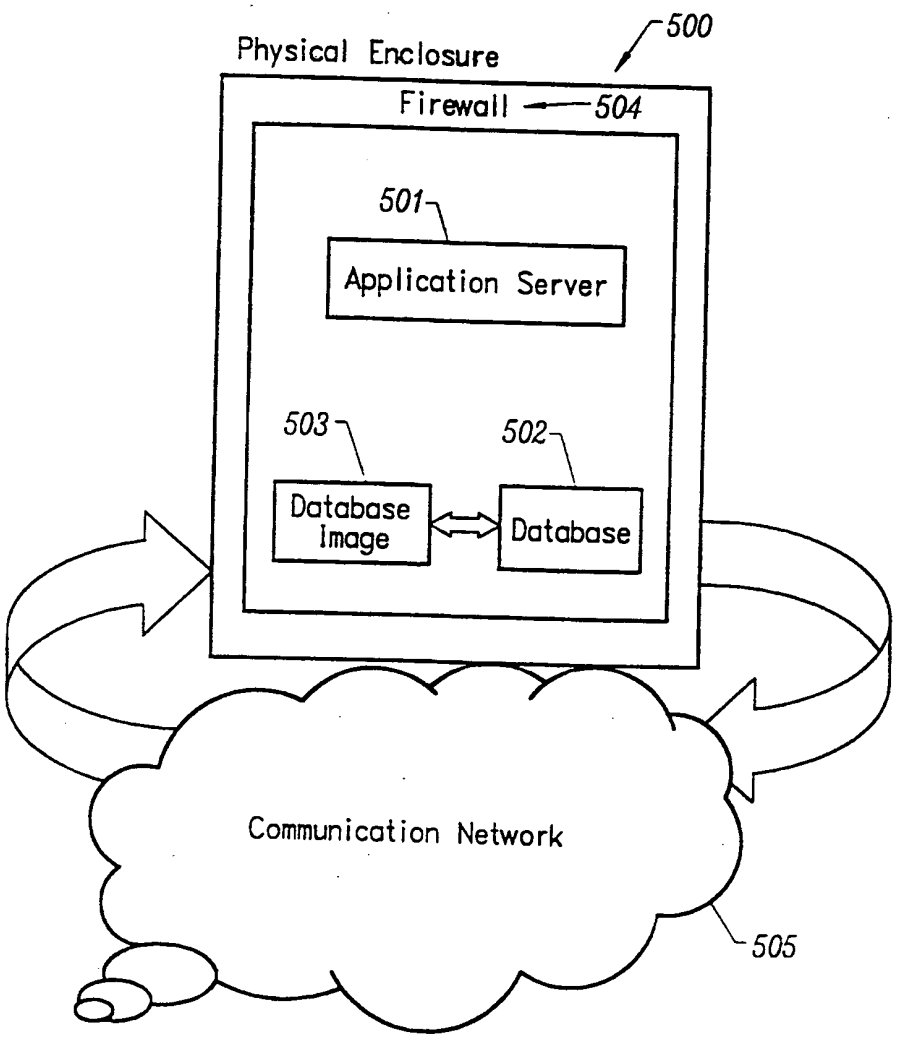

Physical Enclosure
500
Firewall
504
501
Application Server
503
502
Database Image
Database
Communication Network
505

FIG. 5

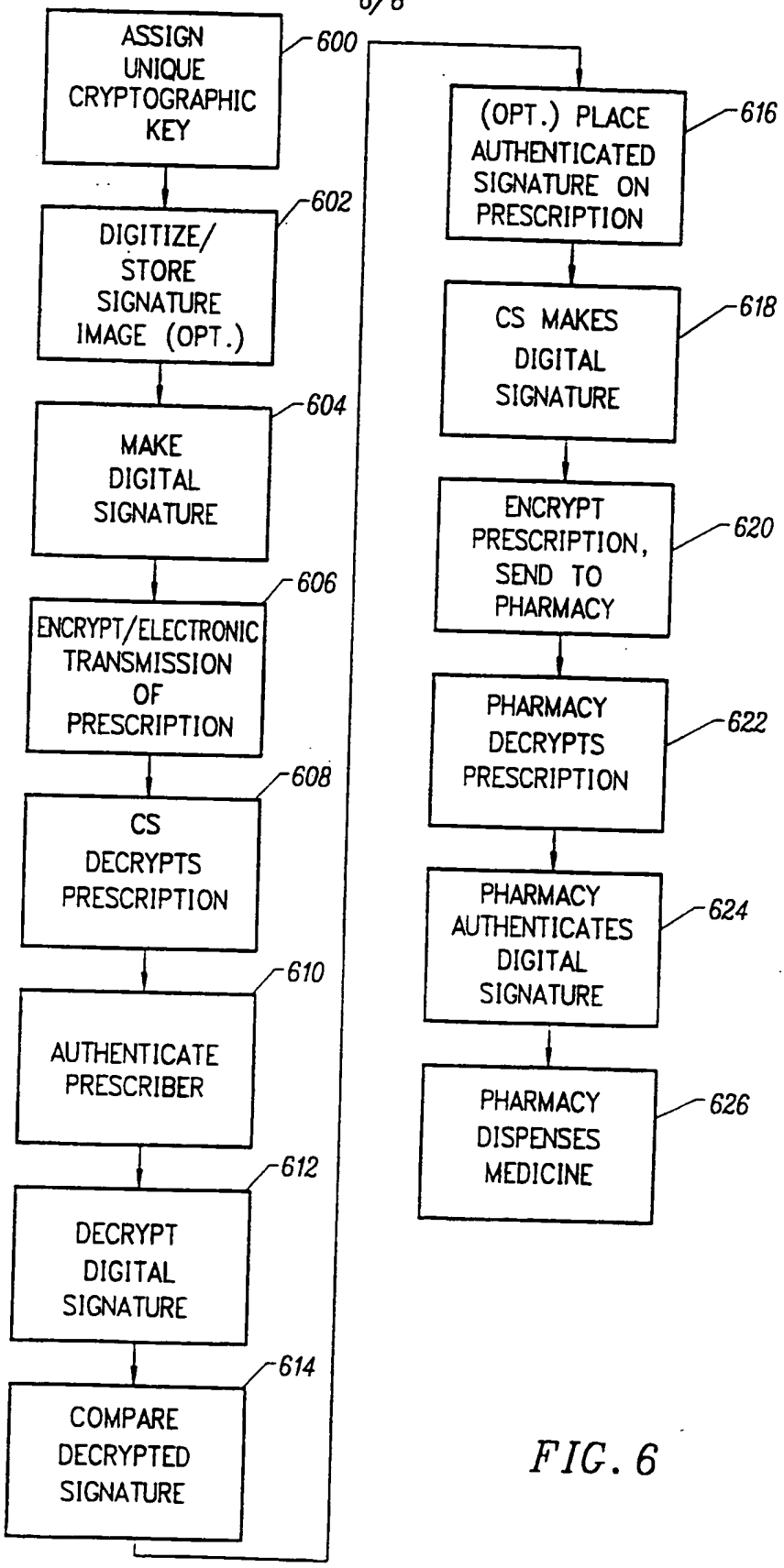

ASSIGN UNIQUE CRYPTOGRAPHIC KEY
600
DIGITIZE/ STORE SIGNATURE IMAGE (OPT.)
602
MAKE DIGITAL SIGNATURE
604
ENCRYPT/ELECTRONIC TRANSMISSION OF PRESCRIPTION
606
CS DECRYPTS PRESCRIPTION
608
AUTHENTICATE PRESCRIBER
610
DECRYPT DIGITAL SIGNATURE
612
COMPARE DECRYPTED SIGNATURE
614
(OPT.) PLACE AUTHENTICATED SIGNATURE ON PRESCRIPTION
616
CS MAKES DIGITAL SIGNATURE
618
ENCRYPT PRESCRIPTION, SEND TO PHARMACY
620
PHARMACY DECRYPTS PRESCRIPTION
622
PHARMACY AUTHENTICATES DIGITAL SIGNATURE
624
PHARMACY DISPENSES MEDICINE
626

FIG. 6

INTERNATIONAL SEARCH REPORT

Ir. ational Application No
PCT/US 00/20267

A. CLASSIFICATION OF SUBJECT MATTER
IPC 7 G06F1/00

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
IPC 7 G06F H04L

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)
EPO-Internal, WPI Data, PAJ, INSPEC, IBM-TDB

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	WO 98 00947 A (ALLSOFT DISTRIBUTING INC) 8 January 1998 (1998-01-08)	1,2,5,6
A	page 5, line 8 -page 11, line 15 page 13, line 22 -page 20, line 23 page 40, line 28 -page 53, line 26 figures 1,2	3,4,7,8, 10,22, 24-26, 45-49, 51,52,55
	-/--	

[X] Further documents are listed in the continuation of box C.

[X] Patent family members are listed in annex.

° Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
28 November 2000	05/12/2000

Name and mailing address of the ISA	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Tx. 31 651 epo nl, Fax: (+31-70) 340-3016	Jacobs, P

Form PCT/ISA/210 (second sheet) (July 1992)

INTERNATIONAL SEARCH REPORT

In ational Application No
PCT/US 00/20267

C.(Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT

Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	US 5 825 884 A (ZDEPSKI JOEL WALTER ET AL) 20 October 1998 (1998-10-20) abstract column 3, line 9 -column 8, line 21 figures 1-6	1-8,10, 22, 24-26, 45-49, 52,54,55
A	US 5 781 632 A (ODOM GREGORY GLEN) 14 July 1998 (1998-07-14) abstract column 4, line 35 -column 8, line 45	1-8,10, 22, 24-26, 47,55
A	US 5 737 539 A (EDELSON JONATHAN ET AL) 7 April 1998 (1998-04-07) cited in the application abstract column 9, line 5 -column 18, line 7 column 26, line 55 -column 30, line 57 column 43, line 48 -column 53, line 50	1,2,8,9, 11-16, 18-22, 27-41, 51,55
A	EP 0 722 236 A (PITNEY BOWES) 17 July 1996 (1996-07-17) abstract claim 1	1,2,4-6

Form PCT/ISA/210 (continuation of second sheet) (July 1992)

INTERNATIONAL SEARCH REPORT

Information on patent family members

In .ational Application No
PCT/US 00/20267

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
WO 9800947 A	08-01-1998	US 6041123 A	21-03-2000
		AU 3591997 A	21-01-1998
US 5825884 A	20-10-1998	EP 0847649 A	17-06-1998
		JP 11513159 T	09-11-1999
		WO 9800972 A	08-01-1998
US 5781632 A	14-07-1998	NONE	
US 5737539 A	07-04-1998	AU 3972295 A	23-05-1996
		BR 9509357 A	30-12-1997
		CA 2201311 A	09-05-1996
		EP 0800680 A	15-10-1997
		JP 10508131 T	04-08-1998
		WO 9613790 A	09-05-1996
EP 0722236 A	17-07-1996	US 5621795 A	15-04-1997
		CA 2165695 A	28-06-1996
		JP 8254047 A	01-10-1996